

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.



[RESEARCH](#)

[PRODUCTS](#)

[INSIDE DELPHION](#)

[Log Out](#) | [Work Files](#) | [Saved Searches](#) | [My Account](#) | [Products](#)

[Search: Quick/Number](#) | [Boolean](#) | [Advanced](#)

The Delphion Integrated View

Buy Now: ☒ PDF | [More choices...](#)

Tools: Add to Work File: [Create new](#)

View: INPADOC | Jump to: [Top](#) | Go to: [Derwent...](#)

Title: JP6324972A2: LAN STATION PERSONAL COMPUTER AND SECURITY PROTECTION METHOD

Country: JP Japan
Kind: A

Inventor: DAYAN RICHARD A;
 LE KIMTHANH D;
 MITTELSTEDT MATTHEW T;
 NEWMAN PALMER E;
 RANDALL DAVE L;
 RUOTOLO LISA A;
 YODER JOANNA B;

Assignee: INTERNATL BUSINESS MACH CORP <IBM>
[News, Profiles, Stocks and More about this company](#)

Published / Filed: 1994-11-25 / 1993-07-23

Application Number: JP1993000202015

IPC Code: G06F 13/00; G06F 1/00; H04L 12/28;

Priority Number: 1992-09-17 US1992000947019

Abstract:

PURPOSE: To provide a LAN station personal computer and a security protection method.

CONSTITUTION: In a method for protecting a system from an attack on a network to which a LAN station belongs and whose security is protected and in a medialess personal computer system work station (defined as LAN station here), a flag bit showing whether access to the specified security protection mechanism of the system is possible or not during a power on self test is set in a memory in the system, a procedure for obtaining a program for system constitution setting, which is stored in the network, is shown for guiding, a changing and eliminating a password used in the LAN station and password data is prevented from being transmitted on the network.

COPYRIGHT: (C)1994,JPO

INPADOC Legal Status: None [Buy Now: Family Legal Status Report](#)

Designated Country: DE FR GB

Family: [Show 4 known family members](#)

Other Abstract Info: DERABS G94-057592



[Nominate this for the](#)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平6-324972

(43) 公開日 平成6年(1994)11月25日

(51) Int.Cl. ⁵	識別記号	序内整理番号	F I	技術表示箇所
G 0 6 F 13/00	3 5 4 Z	7368-5B		
1/00	3 7 0 E			
H 0 4 L 12/28		8732-5K	H 0 4 L 11/ 00	3 1 0 Z

審査請求 有 請求項の数 3 F D (全 19 頁)

(21) 出願番号 特願平5-202015

(22) 出願日 平成5年(1993)7月23日

(31) 優先権主張番号 07/947, 019

(32) 優先日 1992年9月17日

(33) 優先権主張国 米国 (US)

(71) 出願人 390009531

インターナショナル・ビジネス・マシーンズ・コーポレーション
INTERNATIONAL BUSINESS MACHINES CORPORATION

アメリカ合衆国10504、ニューヨーク州
アーモンク (番地なし)

(72) 発明者 リチャード・エイ・ダイアン

アメリカ合衆国 33487 フロリダ州・ボカラトン73ストリート 830 エヌ・イー

(74) 代理人 弁理士 合田 潔 (外2名)

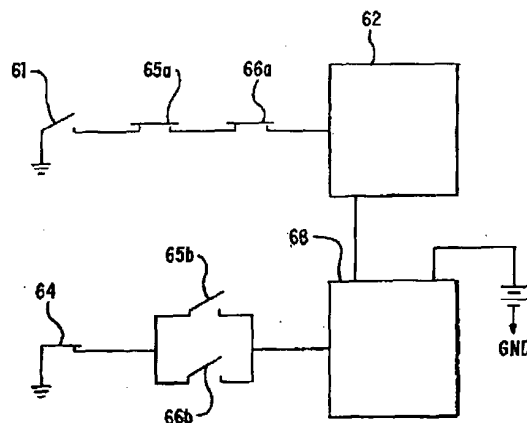
最終頁に続く

(54) 【発明の名称】 LANステーション・パーソナル・コンピュータ及び機密保護方法

(57) 【要約】

【目的】 LANステーション・パーソナル・コンピュータ及び機密保護方法を提供する。

【構成】 LANステーションが属し、機密保護を施されたネットワークに対する攻撃からシステムを保護する方法と、メディアレス・パーソナル・コンピュータ・システム・ワークステーション (ここではLANステーションと定義されている) で、パワーオン・セルフテスト中に、システムの特定の機密保護機構へのアクセスが可能であるかどうかを示すフラグ・ビットがシステム内のメモリにセットされ、ネットワークに記憶されたシステム構成設定用プログラムを、該LANステーションで使用するパスワードの導入、変更、削除の為、取得する手順を示し、パスワード・データをネットワーク上に送出する事を回避する。



【特許請求の範囲】

【請求項1】 ネットワークとデータを交換し、システムにアクセス可能なデータを不正なアクセスから保護する能力を有するLANステーション・パーソナル・コンピュータ・システムであって、

コマンドを入力するためのユーザ入力装置と、通常閉じているカバーと、

カバー錠の鍵の所有者以外のカバー内部へのアクセスを拒絶するため、上記のカバーを機密保護状態に維持するためのカバー錠と、

パスワード・データを受取り、記憶し、選択して動作可及び動作不可の状態にできるように上記のカバー内に取り付けられた消去可能なメモリ要素と、

上記のカバーの内部に取り付けられ、カバーの中からのみアクセス可能で、上記の消去可能メモリ要素を動作可及び動作不可状態にセットするために上記の消去可能メモリ要素に接続して動作するオプション・スイッチと、

上記のカバー内に取り付けられ、上記のメモリ要素の動作可及び動作不可状態を区別することにより、システムにアクセス可能な少なくとも特定レベルのデータのアクセスを制御するため及び上記のユーザ入力装置を通してユーザの入力により上記の消去可能メモリ要素に記憶されたパスワード・データの変更を可能にするため、上記のユーザ入力装置と上記の消去可能メモリ要素に接続して動作するシステム・プロセッサと、

上記のカバー内に取り付けられ、パーソナル・コンピュータ・システムの動作のためのプログラムを記憶し、上記のシステム・プロセッサと接続して動作する読み取り専用メモリ（ROM）装置と、

そのパーソナル・コンピュータ・システムが属しているネットワークを通してアクセス可能な複数の出所の中の選ばれた一つからオペレーティング・システムの初期導入を可能にするため、上記のROM装置に記憶された優先づけられた初期導入プログラムと、

そのパーソナル・コンピュータ・システムが属しているネットワークを通してアクセス可能で、そのパーソナル・コンピュータ・システムの通常のユーザと承認されていないユーザにはアクセスできないように、またシステム・オーナーと承認されたユーザには、

(a) 上記の複数の出所のグループの番号と優先順位を指定することによって上記の優先づけられた初期導入プログラムを選択して変更し、

(b) 上記の入力装置を通して、ユーザの入力により上記の消去可能メモリ要素に記憶されたパスワード・データを選択して変更する、ようにプログラムされた機密保護ユーティリティ手段を備えるパーソナル・コンピュータ・システム。

【請求項2】 上記の消去可能メモリ要素が電気的に消去可能なプログラム可能読み取り専用メモリ装置である請求項1に記載のパーソナル・コンピュータ・システム

ム。

【請求項3】 文字のユーザ入力のための鍵盤と、通常閉じているカバーと、

カバー内に取り付けられ、パーソナル・コンピュータ・システムの動作中、プログラムの実行とデータの処理のため、鍵盤と接続して動作するシステム・プロセッサと、

上記のカバー内に取り付けられ、パーソナル・コンピュータ・システムの動作のためのプログラムを記憶し、上記のシステム・プロセッサと接続して動作する読み取り専用メモリ（ROM）装置と、

複数の出所の中の選ばれた一つからオペレーティング・システムの初期導入を可能にするため、上記のROM装置に記憶された優先づけられた初期導入プログラムと、

パスワード・データを受け取り、記憶し、選択して動作可及び動作不可の状態にできるように上記のカバー内に取り付けられた消去可能なメモリ要素とを備えるLANステーション・パーソナル・コンピュータ・システムの機密保護機構の管理を容易にするための方法であって、

そのパーソナル・コンピュータ・システムが属しているネットワークを通してアクセス可能で、そのパーソナル・コンピュータ・システムの通常のユーザと承認されていないユーザにはアクセスできないように、またシステム・オーナーと承認されたユーザには、上記の複数の出所のグループの番号と優先順位を指定することによって、上記の優先的初期導入プログラムを選択して変更することを可能にするために記憶された機密保護ユーティリティ・プログラムを使用し、それから、

そのパーソナル・コンピュータ・システムが属しているネットワークを通してアクセス可能で、そのパーソナル・コンピュータ・システムの通常のユーザと承認されていないユーザにはアクセスできないように、またシステム・オーナーと承認されたユーザには、上記の入力装置を通して、ユーザの入力により上記の消去可能メモリ要素に記憶されたパスワード・データを選択して変更することを可能にするために記憶された機密保護ユーティリティ・プログラムを使用することを含む機密保護方法。

【発明の詳細な説明】

【0001】 この発明は1992年5月27日付けで米国に出願し、この発明との関連出願である米国特許出願番号889, 324及び889, 325に記載されている発明と関連している。

【0002】

【産業上の利用分野】 この発明はパーソナル・コンピュータ・システム、特にワークステーションとしてローカル・エリア・ネットワークで使用され且つネットワーク内に保持され、また該システムで取扱い可能なデータのアクセス制御を可能にする機密保護機能を有するシステムと関連している。

【0003】

【従来の技術】一般にパーソナル・コンピュータ・システム及び特にIBMパーソナル・コンピュータは今日の近代社会における多くの分野にコンピュータ・パワーの利用を普及させた。パーソナル・コンピュータ・システムは通常次のように定義することが出来る。「単一のマイクロプロセッサと付随する揮発性又は不揮発性メモリを有する1つのシステムユニット、1つのディスプレイ・モニタ、鍵盤、一つ又はそれ以上のディスク装置、固定ディスク記憶装置及びオプションのプリンタによって構成される卓上型、床置き又は携帯用のマイクロコンピュータ」これらのシステムを他と区別する特徴の1つは上述の構成部分を互いに電氣的に接続するためのマザーボード（システム・ボードとして知られており、また本明細書でも折りにふれてシステム・ボード、システム・プレーナ、プレーナと述べられている）を使用していることである。これらのシステムは主として個人ユーザ向けに独立した計算能力を提供するように設計されており、また個人や小規模ビジネスによる購買のため価格は低く設定されている。このようなパーソナル・コンピュータ・システムの例としてはIBM PERSONAL COMPUTER AT及びIBM PERSONAL SYSTEM/2 モデル25, 30, 35, 40, L40SX, 50, 55, 56, 57, 65, 70, 80, 90, 95がある。

【0004】これらのシステムは2つの一般的系列に分類される。第1の系列は、これは通常系列1のモデルとして照会されているのであるが、IBM PERSONAL COMPUTER AT及びその他「IBM互換機」によって例証されるバス・アーキテクチャを使用している。第2の系列は、これは通常系列2のモデルとして照会されているのであるが、IBM PERSONAL SYSTEM/2 モデル57から95によって例証される、IBMのマイクロチャンネル・バス・アーキテクチャを使用している。

【0005】初期の系列1のモデルはシステム・プロセッサとして広く使われたINTEL 8088又は8086マイクロプロセッサを典型的に使用した。その後の特定の系列1及び系列2のモデルは、低速のINTEL 8086マイクロプロセッサと類似の動作をさせるために実モード(Real Mode)で動作し或いはアドレス範囲のある種のモデルに対して1メガバイトから4ギガバイトへ拡張する保護モードで動作し得る高速のINTEL 80286, 80386, 及び80486マイクロプロセッサを使用している。本質的に80286, 80386及び80386プロセッサの実モード機構は8086及び8088マイクロ・プロセッサ用に書かれたソフトウェアに対してハードウェアの互換性を提供している。

【0006】IBMパーソナル・コンピュータのような最も初期のパーソナル・コンピュータから始まって、ソフトウェアの互換性は最重要事項として考えられてきた。この最終目標を達成するために、「ファームウェア」として知られるシステム・レジデント・コードの隔

離層がハードウェアとソフトウェアの間に確立された。このファームウェアがユーザの適用業務プログラム／オペレーティング・システムと装置間のインターフェースを提供しハードウェア装置の諸特徴に係るわずらわしさからユーザを開放した。最終的には、該コードは基本入出力システム(BIOS)の中に組み込まれ、ハードウェアの特性から適用業務プログラムを隔離すると同時に新しい装置をシステムに追加することが許されるようになった。

10 【0007】BIOSが装置に対する中間インターフェースをデバイス・ドライバに提供すると同時にデバイス・ドライバをそれぞれのハードウェア装置の性質に依存する事から解放したためBIOSの重要性は、直ちに明白となった。BIOSはシステム上不可欠な部分であり、システム・プロセッサに入出力されるデータの動きを制御するため、システム・プレーナ上に常駐し読みだし専用メモリ(ROM)の形で客先へ出荷された。例えば、最初のIBMパーソナル・コンピュータにおけるBIOSはプレーナ・ボード上のROM 8Kを専有した。

20 【0008】新しいパーソナル・コンピュータ系列が導入されるについて、BIOSは新しいハードウェア及び入出力装置を包含するため更新したり、拡張しなければならなくなって来た。予期されたようにBIOSはメモリ容量を増加することから開始した。例えば、IBM PERSONAL COMPUTER AT 導入の際BIOSは、32Kバイトを必要とするに至った。

30 【0009】今日、技術革新にともなって、系列2のパーソナル・コンピュータはさらに複雑になり、より頻繁に新モデルが消費者に提供されるようになりつつある。技術は急速に変化し、新しい入出力装置がパーソナル・コンピュータに追加されつつあるので、BIOSの変更がパーソナル・コンピュータの開発過程で大きな問題となってきた。例えば、マイクロチャンネル・アーキテクチャでのIBM PERSONAL SYSTEM/2の導入に際して、相当新しいBIOS(新BIOS又はABIOS)が開発された。しかしながら、ソフトウェアの互換性を保つために、系列1のモデルのBIOSが系列2のモデルに含まれなければならなかった。

40 【0010】系列1のBIOSは後に互換BOIS又はCBOISとして知られるようになった。しかしながら、前にIBM PERSONAL COMPUTER ATに関して説明したとおり、わずか32Kバイト ROMがプレーナ・ボードに有るだけであった。幸運にもシステムはROMを96Kバイトに拡張することができた。不幸にしてこれが、BIOSのために使用できる最大容量であることが判明した。そして更に幸運なことにABIOSを追加してもABIOS, CBOIS合わせて96K ROMに縮小することができた。しかしながら、96K ROMの中のほんの僅かな部分しか次の拡張のために残らなかつ

5

た。将来、入出力装置を追加すれば結局はCBIOSとABIOSはROMを使い果たしてしまうと考えられるようになった。かくして新しい入出力技術は簡単にはCBIOSとABIOSの中に組み込めなくなるであろう。

【0011】これらの問題のため、及び系列2のBIOSに対する変更を開発過程のできるだけ遅い時点で行いたいとする要請と相まって、ROMからBIOSの一部を取り去る必要性が生じてきた。これは、BIOSの一部を固定ディスクのような大容量記憶装置に出来るだけディスク上のシステム区画として定義された部分に記憶させることによって達成された。該システム区画にはシステム・リファレンス・ディスクのイメージを記憶させてあり、その中にはシステム構成を確立するための一種のユーティリティ・プログラム及び同等のプログラムが含まれている。

【0012】ディスクには読みとり能力同様書き込み能力もあるのでBIOSの変更がディスク上で可能になった。ディスクはBIOSコードを迅速且つ効果的に記憶する手段を提供する一方、BIOSコードが破壊される確率を著しく増加させた。BIOSはオペレーティング・システムの不可欠の部分であるので破壊されたBIOSは異常な結果をもたらす可能性があり、多くの場合完全な動作不良及びシステムの不動作をもたらすことになる。かくして、正当と認められないBIOSのディスク上での変更を防止する手段が必要であることはきわめて明白になった。

【0013】これが1989年8月25日出願の米国特許出願番号07/398,820、1991年6月4日発行の米国特許第5,022,077号の主題であった。興味ある読者は、ここに公開する発明の理解に役立つべき追加情報として該特許を参照されたい。そして該特許の内容は本発明の完全な理解のため必要な限り本明細書に参考として編入されている。

【0014】IBM PS/2マイクロチャネル・システムの導入の際、入出力アダプタ・ガード及びブレーナからスイッチやジャンパー線が取り除かれた。マイクロチャネル・アーキテクチャによってプログラム可能レジスタが提供され、これによってスイッチやジャンパー線が置き換えられたのである。これにともなって、これらプログラム可能レジスタ又はプログラム可能オプション選択(POS)レジスタを構成させるためのユーティリティが必要とされた。これらのユーティリティ及びその他システムの使用容易性を改良するためのユーティリティはシステム診断プログラムと共にシステム・リファレンス・ディスクに組み込んで各システムに添付して出荷されるようになった。

【0015】最初の使用に先立って、各マイクロチャネル・システムはそのPOSレジスタを初期化する必要がある。例えば、もしそのシステムが新しい入出力カード

6

を差し込み、或いはスロットを変更してシステム・プログラムの起動がなされると、構成エラーが生成表示され、システム起動手順は停止する。そこでユーザはシステム・リファレンス・ディスクを差し込みF1キーを押すよう指示される。そこで「システム構成用ユーティリティ」がシステム構成のためシステム・リファレンス・ディスクから起動される。システム構成用ユーティリティはユーザに必要な操作を指示する。

【0016】もし適切な入出力の記述子ファイル(Descriptor File)がシステム・リファレンス・ディスクに装填されていれば、システム構成ユーティリティは正しいPOS又はシステム構成データを不揮発性メモリに生成する。記述子ファイルには該入出力カードをシステムとインターフェースさせるためのシステム構成情報が含まれている。

【0017】近年における世界的パーソナル・コンピュータの普及と成長にともなう、ますます多くのデータや情報がこのようなシステムに収集され、保存され又は記録されるようになった。これらデータの中には本来機密を要するものも多い。悪用された場合、そのデータは人々を混乱に陥れ、会社は競争力を失い、或いは機密データは恐喝に使われ、或いは人々に対する物理的暴力へ発展しかねない。多くのユーザがデータの機密性と価値を認識すればするほどますます係るデータの悪用を防止する必要がある。ユーザ自身及びそのデータと関連した人々を守るために、ユーザは購入するパーソナル・コンピュータにデータ保護、機密保護機能を必要としている。

【0018】収集され、記録されたデータの機密保護の必要性を認識しているのはユーザだけではない。政府公共機関もまた法律を制定して機密データの保護を実施している。このような政府公共機関として米国政府がある。米国政府はかねてから事の重要性を認識し、それに答えてきた。米連邦政府は機密保護のレベルとそれぞれのレベルに対応する必要事項を定義し、証明機関を設けてパーソナル・コンピュータの製造業者にその製品を提出させ、その製品が各製造業者が主張している機密保護レベルに合致しているかどうか検査している。連邦政府による必要事項の原典は国防総省による「コンピュータ・システム信頼性評価基準(Trusted Computer System Evaluation Criteria) DOS 5200, 28 STD-1982年12月であり、一般に「オレンジ・ブック(Orange Book)」として知られている。米国政府は1992年1月1日に全ての政府関係データは、パーソナル・コンピュータ上では最低、機密保護レベルC-2で処理され、記録されなければならないと法制化した。

【0019】コンピュータ・システム・ハードウェアに関しては、必要事項の本質は保証セクション、必要事項6に「高信頼機構は、いたずらや承認されていない変更

から恒常的に保護されなければならない。」と記述されている。更に発展して、パーソナル・コンピュータは様々な方法により、様々なアーキテクチャを通じて、ネットワークに組み込まれるようになった。ある特定のこれらのネットワークにおいては、パーソナル・コンピュータはメインフレームとして知られ、大規模データベースを提供し、データを扱う適用業務プログラムの存在場所としての強力なホスト・コンピュータと通信を行う「ダム(dumb)」端末機として主に使われている。

【0020】一方別のネットワークでは、パーソナル・コンピュータが適用業務プログラムや、時にはデータを中央のファイル・サーバ(このファイル・サーバも大容量直接アクセス記憶装置を装備し、比較的迅速なデータの回復速度で動作可能なパーソナル・コンピュータである場合がある)から受取り、処理し、データ入力を受理し、且つファイル・サーバにデータを返送する「スマート(smart)」端末機として使われている。

【0021】更にまた別のネットワーク構成に於いては、パーソナル・コンピュータ群がネットワーク内の1つ又は多数のシステムによって使用可能な資源群を共有している場合もある。これらの資源群としてはプリンタ、スキャナ、モデムなどの周辺機器や互いに資源を共有している1台のパーソナル・コンピュータに直接付属している各種直接アクセス記憶装置上の適用業務プログラム又はデータ・ファイルがある。これらネットワーク構成の多くは、ローカル・エリア・ネットワーク又はLAN(後者 LANが本明細書上の限定用語である)として知られている。

【0022】LANに於けるパーソナル・コンピュータの使用が増大するにつれて、係る状況下で使用される1台あたりの機械の費用は、通常のパーソナル・コンピュータに見られるようなパーソナル・コンピュータの構成要素を取り除く事によって削減し得ると考えられるようになった。この結果、固定ディスクやフロッピー・ディスクのような直接アクセス記憶装置を持たないパーソナル・コンピュータが使用されるようになってきた。このようなシステムはメディアレス・システム或いはLANステーション(本明細書では、後者が限定用語となっている)として知られている。

【0023】ローカル・エリア・ネットワークに於けるパーソナル・コンピュータの使用は、少なくともBIOS機能としての部分に構成された特定の機能を持つような、いかなる典型的パーソナル・コンピュータに対しても、影響をもたらす原因になると考えられる。これらの機能の中には(機密保護レベル C-2を達成目標としている場合) いろいろな機密保護レベルの情報のアクセス管理が含まれるであろう。LANに付随していない単体のパーソナル・コンピュータに関しては、自動構成機能が常識であり、一般に立ち上げ手順の一環として行われ、機密保護機構は最初に述べた関連出願(本発明の

理解に必要な限り参考として本出願に編入されている)の機密保護機構を含む。

【0024】LANに付随したコンピュータに関しては、係る構成動作はコンピュータ内に組み込まれたBIOSの機能として動作し、立ちあげ手順の一環として処理される。しかしながら、LANに接続されたコンピュータの構成動作は、当該コンピュータのパワーオン時点でLANによって自動的に行われる方が望ましい。特に機密保護を必要とするLANに接続されたLANステーションの場合にはシステム・オーナー(System Owner)にとって、係るLANステーションからのLANに対する全ての攻撃への防御が至上命令となる。

【0025】
【発明が解決しようとする課題】 上述の議論を念頭に於いて、本発明はLANステーション・パーソナル・コンピュータ・システム(固定ディスク装置やフロッピー・ディスク装置のようなプログラム記憶媒体を持たない)であって承認されたユーザ又はシステム・オーナー(後述定義のとうり)に対してLAN上でデータが安全にアクセス可能であるようなLANステーションを保証して提供する事を目的とする。

【0026】
【課題を解決するための手段】 LANステーションは機密保護パスワードのような重大なデータのネットワーク上でのいかなる転送も回避する相当な手段を可能にする機密保護機構を必要とする場合がある。その代わりとしてLANステーションで承認されたユーザ又はシステム・オーナーによって直接入力された係る重大データに関してシステムの安全を保証する手段又はシステムに於ける対策がなされている。本発明の目的は、次の手段及び方法によって達成される。

【0027】ネットワークとデータを交換し、システムにアクセス可能なデータを不正な(無許可の)アクセスから保護する能力を有するLANステーション・パーソナル・コンピュータ・システムであって、コマンドを入力するためのユーザ入力装置と、通常閉じているカバーと、カバー錠の鍵の所有者以外のカバー内部へのアクセスを拒絶するため、上記のカバーを機密保護状態に維持するためのカバー錠と、パスワード・データを受取り、記憶し、選択して動作可及び動作不可の状態にできるように上記のカバー内に取り付けられた消去可能なメモリ要素或いは電氣的に消去可能でプログラム可能読み取り専用メモリ要素と、上記のカバーの内部に取り付けられ、カバーの中からのみアクセス可能で、上記の消去可能メモリ要素或いは電氣的に消去可能でプログラム可能読み取り専用メモリ要素を動作可及び動作不可状態にセットするために上記の消去可能メモリ要素或いは電氣的に消去可能でプログラム可能読み取り専用メモリ要素に接続して動作するオプション・スイッチと、上記のカバー内に取り付けられ、上記のメモリ要素の動作可及び動

作不可状態を区別する事により、システムにアクセス可能な少なくとも特定レベルのデータのアクセスを制御するため及び上記のユーザ入力装置を通してユーザの入力により上記の消去可能メモリ要素或いは電気的に消去可能でプログラム可能読み取り専用メモリ要素に記憶されたパスワード・データの変更を可能にするため、上記のユーザ入力装置と上記の消去可能メモリ要素或いは電気的に消去可能でプログラム可能読み取り専用メモリ要素に接続して動作するシステム・プロセッサと、上記のカバー内に取り付けられ、パーソナル・コンピュータ・システム10の動作のためのプログラムを記憶し、上記のシステム・プロセッサと接続して動作する読み取り専用メモリ（ROM）装置と、そのパーソナル・コンピュータ・システムが属しているネットワークを通してアクセス可能な複数の出所の中の一つからオペレーティング・システムの初期導入を可能にするため、上記のROM装置に記憶された優先づけた初期導入プログラムと、そのパーソナル・コンピュータ・システムが属しているネットワークを通してアクセス可能で、そのパーソナル・コンピュータ・システムの通常のユーザと承認されて

いないユーザにはアクセスできないように、またシステム・オーナーと承認されたユーザには、（a）上記の複数の出所のグループの番号と優先順位を指定することによって上記の優先づけた初期導入プログラムを選択して変更し、（b）上記の入力装置を通して、ユーザの入力により上記の消去可能メモリ要素或いは電気的に消去可能でプログラム可能読み取り専用メモリ要素に記憶されたパスワード・データを選択して変更する、ようにプログラムされた機密保護ユーティリティ手段を備えるパーソナル・コンピュータ・システム。

【0028】文字のユーザ入力のための鍵盤と、通常閉じているカバーと、カバー内に取り付けられ、パーソナル・コンピュータ・システムの動作中、プログラムの実行とデータの処理のため、鍵盤と接続して動作するシステム・プロセッサと、上記のカバー内に取り付けられ、パーソナル・コンピュータ・システムの動作のためのプログラムを記憶し、上記のシステム・プロセッサと接続して動作する読み取り専用メモリ（ROM）装置と、複数の出所の中の一つからオペレーティング・システム10の初期導入を可能にするため、上記のROM装置に記憶された優先づけた初期導入プログラムと、パスワード・データを受取り、記憶し、選択して動作可及び動作不可の状態にできるように上記のカバー内に取り付けられた消去可能なメモリ要素或いは電気的に消去可能でプログラム可能読み取り専用メモリ要素とを備えるLANステーション・パーソナル・コンピュータ・システムの機密保護機構の管理を容易にするための方法であって、そのパーソナル・コンピュータ・システムが属しているネットワークを通してアクセス可能で、そのパーソナル・コンピュータ・システムの通常のユーザと承認さ

れていないユーザにはアクセスできないように、またシステム・オーナーと承認されたユーザには、上記の複数の出所のグループの番号と優先順位を指定する事によって、上記の優先的初期導入プログラムを選択して変更することを可能にするために記憶された機密保護ユーティリティ・プログラムを使用し、それからそのパーソナル・コンピュータ・システムが属しているネットワークを通してアクセス可能で、そのパーソナル・コンピュータ・システムの通常のユーザと承認されていないユーザにはアクセスできないように、またシステム・オーナーと承認されたユーザには、上記の入力装置を通して、ユーザの入力により上記の消去可能メモリ要素或いは電気的に消去可能でプログラム可能読み取り専用メモリ要素に記憶されたパスワード・データを選択して変更することを可能にするために記憶された機密保護ユーティリティ・プログラムを使用することを含む機密保護方法。

【0029】

【実施例】これから本発明を添付図面を参照しながら詳細に説明するのであるが、図面では本発明の望ましい具体例が示されているのであり、通常の技術知識を有する人がここで述べる発明を修正しても、本発明の良好な結果が得られる。特定の限定用語が次のように使われている。

【0030】トラステド・コンピューティング・ベース（Trusted Computing Base）—TCB：コンピュータ・システム内に防御メカニズムが完備していること（ハードウェア、ファームウェア及びソフトウェアを含む）、実施する機密保護政策によりこれらを組み合わせる。TCBは1又は多数の要素で構成され、これら要素は共同して製品又はシステム上で統一した機密保護政策を実施する。機密保護政策を正確に実施するためのTCBの能力は、もっぱらTCB内のメカニズムに依存し、またシステム運用員による機密保護関連のパラメータ（例えばユーザの認定）の正しい入力に依存する。

【0031】トラステド・ソフトウェア（Trusted Software）：TCBのソフトウェア部分。

【0032】トラステド・プログラム（Trusted Program）：トラステド・ソフトウェアに含まれるプログラム。

【0033】オープン・プログラム（Open Program）：TCB上で動作するプログラムでトラステド・プログラム以外のもの。

【0034】リファレンス・モニタ・コンセプト（Reference Monitor Concept）：アクセス制御の概念で科目別対象に対する全てのアクセスを調停する概念機械を指す。

【0035】セキュリティ・カーネル（Security Kernel）：リファレンス・モニタ・コンセプトを実施するTCBのハードウェア、ファームウェア、及びソフトウェアの要素。セキュリティ・カーネルは全てのアクセスを調停し、変更されないように防御されており、且つ正しく

検証可能でなければならない。

【0036】トラステッド・コンピュータ・システム (Trusted Computer System) : 一連の重要又は機密の情報を、同時に処理するためにその使用を許可されているハードウェア及びソフトウェアによる保全性を有するシステム。

【0037】システム・オーナー (system Owner) : システム・オーナーはシステムを最初に構成し、機密保護状態にする責任があるユーザのこと。システム・オーナーは最初に且つ更新が必要な都度その構成を管理する。システム・オーナーは特権アクセス・パスワードを管理しその保全に責任を持つ。システム・オーナーは不正アクセス防止用カバード錠の鍵について、その物理的保全性を維持する責任がある。システム・オーナーはまた、全てのシステムの機密保護記録(log)を維持する責任がある。システム・オーナーは試みられる全ての機密保護の侵害を記録しなければならない。システム・オーナーは複数のシステムを受け持つ場合がある。システム・オーナーは、承認されたユーザであり且つ通常のユーザでもあり得ると考えられる。

【0038】機密保護モード (Secure Mode) : 機密保護を構成する諸要素によって、機密防御機能を発動すべくシステム・オーナーが特権アクセス・パスワードをパーソナル・コンピュータ上に正しく導入した状態。

【0039】承認されたユーザ (Authorized User) : 特権アクセス・パスワードを使用する事を承認された全てのユーザ。この人はシステム・オーナーである場合もそうでない場合もある。この人はまた特定のシステム或いは複数システムをセットとして、鍵を保有する場合がある。もしこの人が機密保護に対する侵害からのシステム回復作業に関わる場合は、この人は責任を持って当該侵害の事実をシステム・オーナーに報告しなければならない。承認されたユーザはまた通常のユーザである場合もある。

【0040】通常のユーザ (Normal User) : システム設備を使用する事を承認された全てのシステム・ユーザ。システム構成を変更するため、又は発生した問題を解決するためには、このユーザはシステム・オーナーか承認されたユーザの何れかの援助を必要とする。通常のユーザは承認されたユーザかシステム・オーナー部門の何れかに所属しない限り、特権アクセス・パスワードやカバード錠の鍵を持たない。

【0041】承認されていないユーザ (Unauthorized User) : システム・オーナー、承認されたユーザ又は通常のユーザの何れにも定義されていない人。承認されていないユーザによる機密保護を施したパーソナル・コンピュータの如何なる使用も、不成功に終わったパワーオンを除いて機密保護に対する侵害と考えられ、係る侵害を示す監査用追跡記録が存在しなければならない。

【0042】EEPROM : 電氣的に消去可能でプログ

ラム可能な読み取り専用メモリ。このメモリ技術はハードウェアの論理回路によってデータの変更が可能な不揮発性メモリを提供する。パワーオフの状態でもメモリの内容は失われない。内容は、当該モジュールに適切な制御信号が事前に定義された手順で印加された場合にのみ変更される。

【0043】パスワード記述 (Password Description) : システムは次の2種類のパスワードによって保護される可能性を有する。1 : 特権アクセス・パスワード (Privileged Access Password - PAP)。2 : パワーオン・パスワード (Power On Password - POP)。これらパスワードは互いに独立して使用されるように意図されている。

【0044】PAPはシステム・オーナーに対して初期プログラム導入 (IPL) 用装置起動リスト、パスワード・ユーティリティへのアクセス及びシステム・リファレンス・ディスク・イメージへのアクセスを防止する事によって、防御を提供するように設計されている。

【0045】本発明が関係するネットワーク環境に於いては、装置起動リスト、パスワード・ユーティリティ及びリファレンス・ディスク又はシステム区画へのアクセスは、LANステーションがメディアレスであり、従って係るLANステーションでは直接アクセスの能力を欠いているために、ネットワーク・サーバを通じてのみ行われる。これが本発明の重要な特徴である。

【0046】PAPの存在はPOPを使用している通常のユーザにとって明白である。PAPはサーバを通じてアクセス可能なシステム・リファレンス・ディスク・イメージ上にあるユーティリティ・プログラムによって導入され、変更され、或いは削除される。PAPはもし正しく設定され、入力されれば、システム・オーナーはPOPに優先して、システム全体へのアクセスができることになる。

【0047】POPは、現在の全てのPS/2で稼働しているのであるが、ネットワーク・サーバ或いはネットワーク上の施設に対する如何なる不正なアクセスをも防止するために使用される。更に具体的に添付図面を参照すれば、本発明を具体化するマイクロコンピュータが10 (図1) に図示されている。上述の如く、コンピュータ10はそれに付属したモニタ11、鍵盤12、プリンタまたはプロッタ14を持っている。

【0048】コンピュータ10には図2に示したように、デジタル・データを処理し、記憶するための電力によるデータ処理部及び記憶部を収容し、シャシ19と共にこれらを包み、遮蔽するカバー15がある。

【0049】図2に示された形態において、コンピュータ10には、コンピュータ・システムに関する入出力ケーブルの接続点を拡張し、併せて保護するオプションの入出力ケーブル接続用カバー16がある。少なくともシステム構成部分のいくらかは、シャシ19に固定された

多層プレーナ20（ここではマザーボードまたはシステム・ボードとして記述されている）に収容されており、該多層プレーナは上述のコンピュータ構成部分や、その他付随するフロッピー・ディスク装置、各種の直接アクセス記憶装置、補助カード、ボード類を電気的に接続する手段を提供する。

【0050】シャシ19には、基盤と後部パネルがあり（図2、通常、ケーブル接続カバー16によって外側から覆われている）、磁気或いは光学的ディスク装置、バックアップ用テープ装置類のようなデータ記憶装置を収容するための少なくとも一つの空間をとってある。

【0051】図に示した形態において、上部空間22は、第1サイズの周辺機器（3.5インチの装置として知られているもの）を収容するよう適合している。フロッピー・ディスク装置は、ディスクケットを挿入し、そのディスクケットを使用してデータを受け取り、記録し、引き出す事ができる取り外し可能な媒体を使用した直接アクセス記憶装置として知られているが、通常該上部空間22に収容される。

【0052】しかしながら、ここで述べるLANステーションの場合には、システム10の費用を削減するため、このような直接アクセス記憶装置は提供されない。本発明の上記構造について述べる前に、パーソナル・コンピュータ・システム10の一般的動作についてその要点を再吟味する事は価値があるであろう。

【0053】図3において、本発明によるシステム10のようなコンピュータ・システムの各種構成部分を示すパーソナル・コンピュータのブロック・ダイアグラムが図示されている。このブロック・ダイアグラムには、プレーナ20に収容された構成部分とプレーナと入出力スロット及びその他のパーソナル・コンピュータのハードウェアとの接続が含まれる。システム・プロセッサ32もプレーナに接続されている。如何なるマイクロプロセッサでもCPU32として使用して良いのであるが、一つの適切なマイクロプロセッサとしてインテル社から発売されている80386がある。該CPUは、高速CPUバス34によって、バス・インターフェース制御部35、シングル・インライン・メモリ・モジュール（SIMMs）として示される揮発性ランダム・アクセス・メモリ（RAM）36及びCPU32に対する基本入出力動作の命令群を記憶するBIOS ROM38と接続されている。

【0054】BIOS ROMは、入出力装置とマイクロプロセッサ32のオペレーティング・システムとの間を整合させるために使用されるBIOSを含む。BIOS ROM38に記憶される命令群は、BIOSの実行時間を減少させるためにRAM36に複写する事ができる。

【0055】当該システムはまた、すでに一般的になっているように、システム構成及び実時間クロック（RT

C）68（図3）に関するデータを受信し、記憶する電池バックアップ型不揮発性メモリ（CMOS RAM及びNVRAMとして知られている）を有する回路部を持つ。

【0056】本発明は、今後図3のシステム・ブロック・ダイアグラムを特に参照しながら記述するのであるが、本発明による機械装置及び方法は、プレーナ・ボードの他のハードウェア構成でも使用され得る様に意図されている事を初めに理解されたい。例えば、当該システム・プロセッサはインテル社の80286または80486マイクロプロセッサでもかまわない。

【0057】図3に帰って、CPUバス（bus）34は（データ、アドレス、制御部を含む）またマイクロプロセッサ32と数値演算用コプロセッサ（MCP）39との接続を行い、更に場合によっては、小型コンピュータ・システム・インターフェース（SCSI）制御部40との接続も行う。もし存在していれば、SCSI制御部40は、コンピュータの設計及び操作の分野の技術を有する人には自明のことではあるが、読みとり専用メモリ（ROM）41、RAM42、及び図の右側に表示された入出力接続端子によって容易となる各種の内部または外部装置と接続可能である。

【0058】SCSI制御部40は、固定または取り外し可能な媒体の電磁氣的記憶装置（固定またはフロッピー・ディスク装置として知られている）、電気光学的、テープ及びその他の記憶装置を制御する記憶制御部として機能する。上述の通り、係る装置類は一般的に経済的理由によりLANステーション・パーソナル・コンピュータでは削除されており、同じ理由によりSCSI制御部も削除される場合がある。しかしながら、LANステーションの購入の際将来のシステムの格上げを意図する場合があるので、SCSI制御部のような要素或いはDASDの為の空間などはしばしば用意されている。

【0059】バス・インターフェース制御部（BIC）35は、CPUバス34と入出力バス44とを連結している。バス44によって、BIC35は更に多くの入出力装置またはメモリ（図示されていない）を接続するためのマイクロチャンネル・アダプタ・カード45を収容するための複数の入出力スロットを有するマイクロチャンネル・バスのようなオプション機構用バスと連結している。

【0060】入出力バス44はアドレス、データ、及び制御部を含む。一般にLANステーション・システムに於いては、1枚のオプション・カード45が当該システムとその属するネットワークとを接続する接続点を提供する。入出力バス44と連結して、グラフィック情報（48）や画像情報（49）を記憶するビデオRAM（VRAM）に付随するビデオ信号処理部46など各種の入出力部がある。

【0061】プロセッサ46で変換されたビデオ信号

は、デジタル・アナログ変換器(DAC)50を通してモニタまたはその他のディスプレイ表示装置へ送られる。ここでは、VSP46を直接自然画像入出力と照会されている装置と接続する対応もなされている。これらの装置は、ビデオ・レコーダ/プレーヤ、カメラ等の形をとる場合がある。入出力バス44はまた、デジタル信号処理部(DSP)51と連結されており、そのDSP51はDSP51とその処理に関係したデータによる信号を処理するためのソフトウェア命令群を記憶する命令RAM52とデータRAM54とを付随して持っている。DSP51は、音声制御部55による音声入出力の処理とアナログ・インターフェース制御部56によるその他の信号の処理を行う。

【0062】最後に、入出力バス44は入出力制御部58及びそれに付随した電氣的に消去可能でプログラム可能な読みとり専用メモリ(EEPROM)59と連結し、該EEPROMによって入力及び出力がフロッピー・ディスク装置、プリンタまたはプロッタ14、鍵盤12、マウスまたは指示器(図示されていない)、及びシリアル・ポートによる手段を含む一般周辺装置と交換される。EEPROMはここで述べる機密保護機能の一部を担当する。

【0063】ここで述べるように、パーソナル・コンピュータ・システムの機密保護という特定の目的を達成するために、パーソナル・コンピュータ・システム10は、その内部に選択して動作可能状態にしたり、動作不能状態にしたりでき、動作可能状態の時特権アクセス・パスワードを受け取って記憶するように、消去可能なメモリ要素を持っている。消去可能なメモリ要素は、電氣的に消去可能でプログラム可能な読みとり専用メモリ又は上記EEPROM59(図3)の1フィールド又は部分であることが望ましい。システムはまた、オプション又は機密保護スイッチをそのカバーを内部に設け、該メモリ要素の中の使用されたフィールド又は部分を動作可能又は動作不能状態にする為に、消去可能メモリ要素59と接続して動作するようになっている。該オプション・スイッチ(本開示では機密保護スイッチとも呼ばれる)は、例えば、システム・プレーナ上のジャンパで、プレーナにアクセス可能な人によって、手作業で2種類の状態を設定できるものであっても良い。

【0064】一つの状態(ここでは書き込み可能又はロック解除と呼ぶ)では、EEPROM59はここで述べるように動作可能状態に設定され、PAPを記憶できるようになっている。書き込み可能状態では、PAPはEEPROMに書き込み、変更され、削除される。その他の或いは動作不能状態では、(ここでは、書き込み不可又はロック状態という)EEPROMのPAP記憶能力は、動作不能に設定されている。この発明によれば、LANステーションの製造時の初期状態は、パワーオン時にシステムを機密不保護の状態に設定してある。

【0065】システムが機密保護状態になるためには、システム・オーナーは、施錠されたカバーを開けて、システム・プレーナ20にある機密保護スイッチの状態を意図的に変更し、機密保護パスワードの活性化を可能にし、システムを機密保護システムに成らしめなければならない。更に、システム・オーナー又は承認されたユーザは、手順を追って特別の処理を実行してPAPの導入をしなければならない。係る処理とそれに適応するシステムの特徴が、本発明の焦点である。

【0066】上述のように、システム10はまた、図4の68に示すように、消去可能なメモリ能力、すなわち電池による不揮発性CMOS RAM、及び実時間クロック(RTC)を持つ第2の部分の有する。CMOS RAM又はNVRAMは、本発明によれば、システム10のパワーオン時にPAPの成功の入力に関するデータを含むシステム構成を表示するデータを記憶する。少なくとも1個の不正な解錠の検出用スイッチ(図4、5、6)が用意され、カバー内に取り付けられ、カバーが開いている事を検出し、該不正な解錠検出用スイッチの動作にตอบสนองしてメモリを消し去ったり或いはメモリ内に記憶されている特定のデータを設定したりするためのCMOS RAMと接続して動作するようになっている。

【0067】システム・プロセッサ32は、本発明によれば、EEPROM59とCMOS RAM68に接続して動作し、メモリのPAP記憶能力の動作可又は動作不可の状態を区別し、正しいユーザすなわち記憶されている特権アクセス・パスワード(PAP)による入力又は無入力を区別することによってシステム内に記憶された少なくとも特定のレベルのデータへのアクセスを一部制御するよう機能する。上記オプション・スイッチを操作する事によって、システム及びそれに関わるネットワークの操作員(具体的には、機密保護を維持し監督する立場にある人)は、EEPROMの状態を動作可或いは動作不可になるように選択してシステムを機密保護動作或いは機密保護でない動作になるよう選択する事ができる。もし機密保護動作が要請され実施する事になれば、システム・オーナーはPAPを入力しなければならない。

【0068】ここで開示したように、この発明による機密保護業務に対応するシステムは、2つの別々の不揮発性で消去可能なメモリ要素、EEPROM及びCMOS RAMを有する。この事は、本発明の時点で一部実施されたのであるが、PAPの状態の表示やPAPの正しい入力は少なくとも無許可でカバーを開ける事の可能性と同様に、非常に多くの回数消去、書き込みの必要があるにも関わらずEEPROMは、消去、書き込みサイクルの回数に関して寿命が限られているので、このようにした。このために、ここで述べる機能は、現在の技術に対応するため第1及び第2の消去可能なメモリ要素に分割されている。

【0069】しかしながら、本発明は、これら2形態の

関連データは、もし技術が許すならば、或いはもし設計者が係る選択に伴う制限を受け入れるならば、単一の消去可能なメモリ要素に記憶させる事を意図している。

【0070】ここで図4から図7までの概略図を参照する事によって、本発明に係る特定のハードウェア機構がより具体的に述べられている。図4は、一般的な電源制御又は「ON/OFF」スイッチ61、一般的電源62、主カバー15及びケーブル接続カバー16の様なカバーの開放又は除去にตอบสนองして導通状態を変えるスイッチ、およびカバー錠スイッチ64の特定の関係を示して

10 いる。カバーの開放又は除去の状態を変えるスイッチは、本発明の図でいえば、2つある。すなはち、主カバー15の除去に対してตอบสนองするスイッチ65（図4、5、6）及びケーブル接続カバーの除去にตอบสนองするスイッチ66である。

【0071】各スイッチは2つの部分からなっている、1つは通常開（それぞれ65a、66a）、もう1つは通常閉（それぞれ65b、66b）である。第2のスイッチは、ケーブル接続カバー16がそうであるように、オプションである。しかしながら、本明細書での注意深い考察によって明らかなように、オプション・カバーとスイッチは、システムに対するより完全な機密保護を保証する。

【0072】通常開状態になっているカバー・スイッチ65と66の接点群は、主電源スイッチ61と電源62に直列に接続されている（図4）。従って、もしカバーをはずしてシステム10の電源を入れようとすると、当該接点群65aと66aは開状態となりシステムの動作を防止する。カバーをしたままであると、当該接点群は閉じ状態になっているため、正常なシステム動作が開始

30 され得る。

【0073】通常閉状態のカバー・スイッチ65と66の接点群は、カバー錠スイッチ64及びCMOS RAM68と直列に接続されている。当該通常閉状態の接点65bと66bは、カバー15及び16の存在によって開状態となり、これらカバーの除去によって閉状態となる。

【0074】カバー錠スイッチ64は、コンピュータ・システム10に一般的に提供されているカバー錠を施錠する事によって、通常閉状態となる。これら3種類の接点群は、電流のグラウンドへの交代経路もしくはCMOS RAMの付勢化の一部分を形成しており、カバー錠が施錠状態になっているシステムの状態でカバーが不正に除去されたために、付勢化が失われれば、該メモリの特定区分を特定の状態（全て「1」で埋めるなど）に設定する効果を有する。

【0075】当該メモリはPOST(Power On Self Test)によってチェックされているため、当該メモリ区分を特定の状態にする事は、構成エラー信号を発生し、システム・オーナーに対して機密保護の侵害（成功か不成功か

は別にして）が試みられた事を警報する事になる。

【0076】メモリ区分を特定状態に設定するためには、オペレーティング・システム起動のための事前に記憶されたパスワードが必要である。すなはち、本明細書で別途開示したように、オペレーティング・システムの起動には、正しいPAPの入力が必要である。一般カバー錠スイッチ64と主カバースイッチ65は、主カバー上にある錠に関連して適切に位置づけられるように、前面カード・ガイド部69（図2、6）に取り付ける事が望ましい。前面カードガイド部は、コンピュータ・システム・フレーム上で、カバー15が存在し、然るべき位置に置かれて、システムのカバーとして機能しているとき、カバースイッチ65の発動レバー70が、直立前面フレーム部の開口部に突き出るような位置に取り付けられている。

【0077】ケーブル・カバースイッチ66は、システム・フレームの後部パネルに取り付けられ、ケーブル・カバー16上に取り付けられたラッチ部によって発動され且つ主カバー15の場合と同様に手操作で錠が回転できるように位置づける事が望ましい。オプションのケーブル・カバー16が使用されているとき、（完全なシステムの機密保護が必要な場合）、カバーを後部パネルに固定する事によって該、ラッチ部によって通常開の接点66aが閉状態になるように、また通常閉の接点66bが開状態になるように設定される。

【0078】上述或いは後述の機密保護・保全機構は、前に提案されたパーソナル・コンピュータの機密保護機構、パワーオン・パスワード（POP）とは独立して動作する。係る追加の機密保護・保全機構は、オレンジ・ブックのような当面する規定のもとで、システム認定の為の安全な装置を提供する。

【0079】もう一つのパスワードがシステムを機密保護状態にするために必要である。その新しいパスワードがここで言う特権アクセス・パスワード（PAP）である。以前のパーソナル・コンピュータ・システムとの互換性を維持するために、POPも依然として使用できるようになっている。

【0080】パスワード保護はシステム・ハードウェア：EEPROM、機密保護スイッチ及びカバー・スイッチ、ファームウェア、POST及びシステム・ソフトウェア・パスワード・ユーティリティ、によって実行される。一度PAPが導入されると、システムは機密保護モードになる。PAPはEEPROMに保存される。PAPのバックアップ用コピーもEEPROMに保存される。このKOT0は、PAPの導入、変更、削除の最中に電源断が発生して、PAPが偶発的に消失するのを防ぐために行われる。

【0081】POP及びPAP（もし導入されていれば）の正当性を証明する少なくともいくつかの特定ビットがNVRAMに記憶される。NVRAM及びEEPROM

OMに保持されたデータの変更は互いに独立して行われる。EEPROMの中の2ビットが当該変更手順のどこで電源断が発生したかをPOSTに対して知らせ、できればシステム・ボードの交換の事態から再生させる機関として使われる。パスワード・ユーティリティは変更表示フィールド、PAPへアクセスする際に使われる2ビットの状態表示機関、を維持する。

【0082】もしもパスワードの変更中に電源断が発生すれば、電源が再度回復した時POSTが上記状態表示機関をチェックする。(POSTは実際には、全てのパワーオン時点で該状態表示機関をチェックする。)もしPAPの変更が成功すれば、(「00」状態)POSTは処理を続行する。もし変更が電源断の前に開始していれば、(「01」状態)POSTは正当なバックアップPAPの存在をチェックする。もし正当であれば、バックアップPAPを主PAPへ複写する。もしオプション又は機密保護スイッチがロック解除の状態又は書き込み可能状態になっていなければエラーが表示される。この際システム・オーナーは、カバーのロックを解除し、機密保護スイッチの位置を変えなければならない。

【0083】もし主PAPの変更が成功すれば(「10」状態)、システム・リファレンス・ディスクの使用又はシステム区画の起動をしようとする試みを検証するために主PAP(新PAP)を使用する。POSTはバックアップPAPが正しくないと想定し、この場合POSTは主PAPをバックアップPAPに複写する。

【0084】もしバックアップPAPがうまく変更されていれば、(「11」状態)主PAP及びバックアップPAPの両方とも正当であると考えられ、POSTはユーザによるPAPの入力を確認する前に主PAPの正当性を検証する。上述のようにPOPはCMOSメモリの中に維持されている。2ビットがPAPの為のパスワード表示器として使用するためにCMOSメモリに維持されている。1つの表示器はシステムが機密保護モード(PAPが導入済み)にある事を示すために使用される。第2の表示器はPAPが最初のパワーオン時(コールド・ブート - Cold Boot)には正しく導入されていた事を示すために使われる。

【0085】これら2つの表示器は初期化されコールド・ブート時にのみ設定される。IPLに先立って、もしシステム・リファレンス・ディスク又はシステム区画が起動されていなければ、これら表示器は書き込み保護され、該IPLは導入済みPAPの入力が成功することを必要とする。POPとこの表示器の変更はEEPROMに記憶されたPAPの変更と独立して行われる。しかしながら、CMOSメモリの変更は、オペレーティング・システムの導入を許し、回復のため正しいPAPの入力が必要となる機密保護の侵害を表示することができる。

【0086】パスワードに対する不正アクセスを防止す

るため、IPL装置起動リスト、EEPROM CRC、及び全ての表示器は、オペレーティング・システムを起動する初期プログラム導入(IPL)に先立ってロックされる。係る分野を排除するため、POSTはシステムがパワーオフされない限りリセットされない特定のハードウェア・ラッチをセットする。

【0087】POSTの第一段階(最初のパワーオン)のはじめに、POSTはEEPROMがロックされているかどうかチェックする。もしロックされていれば、POSTはエラーを表示し、ハードウェアが機能していないとしてシステムを停止する。システム・オーナーは、状況を矯正するため介入し、場合によってはシステム・ボードを取り替えなければならない。

【0088】本発明の一形態に於いて、システムが物理的不正変更を加えられているとき、CMOS RAMの最初の14バイトは影響を受けていない。次のCMOS RAMの50バイトは上で概説したように、全て「1」(バイナリ 1)に設定される。この状況を検出したときPOSTは適当なエラー表示を行う。

【0089】本発明のもう1つの形態に於いては、できるだけ小数のビット数がシステムの物理的不正変更表示として設定される。何れの例に於いても、システム・オーナー/承認されたユーザは、状況の矯正に介入しなければならず、その矯正にはシステム・リファレンス・ディスク又はシステム区画起動のためパスワードを要請された時、PAPの入力が必要であったり、システム・ボードの取り替えが必要であったりする場合がある。もしシステム・オーナーがPAPを忘れたら、当該システム・ボードの取り替えが必要となろう。

【0090】もしPOPを忘れたら、システム・オーナーは上述のようにCMOS RAMの内容を捨てることができ、PAP(もし導入されていれば)を入力してパスワード・ユーティリティを実行するためにシステム・リファレンス・ディスクを起動しPOPを再導入することができる。

【0091】何れのパスワードも未導入のままシステムがパワーオンされた時は、POSTはパスワードを要求するメッセージを出さない。しかしながら、POSTはPAP、バックアップ用PAP、IPL装置起動リスト及び全てのインジケータをロックする。このことは、当該分野への如何なる偶発的或いは悪意のアクセスを防止するために行われる。

【0092】システムがPOPを導入し、PAPを導入しないままパワーオンされた時は、POSTはPOPのチェックサム(Checksum)を検証する。もしチェックサムが合格であれば、POSTはユーザにPOPの入力を要求する。もしチェックサムが不合格であれば、POSTはCMOSにあるPOPを消去し、パスワードの入力を要求しない。

【0093】ネットワーク上の如何なるプログラムの起

動に先立って、PAP、バックアップ用PAP、IPL装置起動リスト、EEPROM CRC及び全てのインデキータはアクセスを防止するためロックされる。システムがPAPを導入し、POPを導入しないままパワーオンされた時は、POSTは状態表示機能の状況をチェックし、更にPAPのパスワードのチェックサム(Checksum)を検証する。もしPAPのチェックサムが合格であれば、POSTは通常の処理を続行する。もしPAPのチェックサムが不合格であれば、エラー表示が行われシステムは停止する。

【0094】この事は、POSTが偶発的にユーザに対して、EEPROMエラーのとき、以前に保護状態にあったシステムへの不保護状態でのアクセスを付与する状況を防止するために行われる。システム・オーナは、介入して状況の矯正をする必要があり、その矯正には場合によっては、システム・ボードの取り替えを要する。

【0095】もしシステムが、正しいPAPと正しいPOPを導入した状態でパワーオンされていれば、POSTはユーザにパスワードの入力を促す。もしPOPが入力されれば、POSTはシステム・リファレンス・ディスク・イメージからの起動をしない。システムは現在のIPL装置リストのみを使用して起動する。

【0096】もしPOPでなくPAPが入力されたら、該ユーザはシステム・リファレンス・ディスク・イメージ(ネットワークに対するアクセスが可能であれば)、或いは正常なIPL装置リストから起動することができる。

【0097】このパワーオン手順の後でシステム・リファレンス・ディスク・イメージの起動がされるように、最初のパワーオン時にPAPの入力が成功したことを知らせるインデキータがセットされる。POSTは再起動のためにパスワードの入力を要求する事はない、従ってPAPには、入力成功のインデキータ及びその保護が必要である。POSTは、何れかのパスワードが正しく入力されたことを確認した後、確認のアイコンを表示することにより該入力を認証する。

【0098】POSTの変更と連結して、パスワード・ユーティリティは、PAPに対するサポートを含まなければならない。該ユーティリティは、PAPの導入、変更、削除をサポートし、オプション・スイッチ或いは機密保護スイッチの位置とこれら3つの機能とは連動している。機密保護スイッチは承認されたユーザがPAPのセットを行おうとするまでは、ロックの位置に止めて置くべきである。その時該ユーザは、システム・カバーを取り除き機密保護スイッチをロック解除(変更)の位置へ動かす必要がある。ここでPAPがセットできるのである。機密保護スイッチがロック解除の位置になっているとき、EEPROMの外にあるハードウェア回路がPAPをEEPROMに書き込む事を許しいる。機密保護スイッチがロックの位置にあるとき、該ハードウェア回

路は、PAPの場所に対する如何なる変更も防止している。機密保護スイッチがロックの位置にあるとき、承認されたユーザがPAPを変更しようとするとき、相当するメッセージが現れる。

【0099】追加の安全機構がパスワード・ユーティリティに組み込まれていて、承認されたユーザがPAPをPOPと等しくセットする事を防止している。PAPをセットしたり変更するとき、該新PAPがシステムの現在のPOPと等しくならないようにチェックがなされている。また、PAPを変更したり削除したりするとき、現在のPAPを知っていなければならない。

【0100】パーソナル・コンピュータ・システムは機密保護スイッチをロックの位置にし、カバーは施錠した状態で出荷されることになっている。このことは、システム・オーナ以外の如何なる人もシステムを機密保護モードにセットできないようにするために行われる。POPと異なり、PAPはハードウェアの操作では消去されない。PAPを忘れたり、未承認のユーザがシステムを機密保護モードにするには、システム・ボードを取り替

えなければならない。

【0101】上述のメモリ要素、スイッチ、及びこれらの相互接続は、名前を付けた構成部分が特に機密保護機構を可能にするコンピュータ・システムの要素であることから、本明細書では「機密保護機構要素」として照会されている。

【0102】機密保護機構を有するLANステーションの通常の動作では、すでに述べたように、LANステーションはパワーオンするとパワーオン・セルフテスト(POWER ON SELF TEST = POST)に入る。POST完了の直前にシステムは遠隔初期プログラム導入(RIPL)能力があることを検出する。RIPLは通常オペレーティング・システムがLAN上のサーバから供給されるようにしたもので、サーバはメディアレス・ワークステーションに対する論理的プログラム起動装置として働く。POSTは係る装置からのLANステーション・プログラムの起動を実行する。POSTによって起動されるソフトウェアが未知であるため、POSTは機密保護機構装置内の全ての保護フィールドをロックする。

【0103】明白なように、LANステーションをネットワーク上機密保護ワークステーションとするためには、PAPをセットする手段がなければならず、更にその手順がシステム・オーナや承認されたユーザにとって保護されなければならない。この結果を達成する事が本発明の焦点であり以後詳細に説明する。

【0104】PAP或いはIPL装置起動リスト・フィールドを導入、変更又は削除するために、本発明により意図された1つの方法によれば、サーバとLANステーションの間に調整がなければならない。更に、LANステーションのNVRAM68の中に遠隔PAP導入フラ

グの為の特別なフィールドを用意する必要がある。R I P Lの出所からシステム・リファレンス・ディスク・イメージ或いは機器構成セット用ユーティリティの起動中、起動されるプログラムは、POSTによって指定された機密保護に関するフィールドの状態を検出する。正常操作の結果として、上述のように、これらがロック状態である事が判ると、システム・リファレンス・ディスク・プログラムは遠隔PAP設定フラグをセットし、LANステーションのパワーオフを行い、そして直ちに再びパワーオンするようにメッセージを発生し、LANステーションでのデータ処理を禁止する処置を取って終了する。

【0105】この時点でLANステーションでの承認されたユーザは、ステーションのパワーオフをし、またすぐにオンにする。POSTは、正常な動作を実行することによって、遠隔PAP導入フラグの状態が変わったことを検出し、機密保護機構装置をロック解除にし、遠隔PAP導入のためのフラグ・セットの変更やリセットを可能にしたまま、サーバからのプログラム起動の正常な動作を続行する。

【0106】サーバに定義されたR I P Lの場所にはリファレンス・ディスク・イメージ或いはシステム構成設定用プログラムが残っているため、そのプログラムが起動され、PAPを導入し、PAPを変更又は削除し、必要ならIPL装置起動リストの変更を行うことを可能にするために、承認されたユーザが、システム以前に機密保護装置の当該フィールドを変更できるようにする。

【0107】係る変更を完了するためには、承認されたユーザはシステムのパワーオフを再度行い、R I P Lに先立ってPOSTが機密保護装置フィールドのロックに戻れるようにメモリがクリアされている事を確認する必要がある。PAPをLANステーションに導入する第2の方法によれば、メディアレス・ワークステーションに論理的プログラム導入装置を提供するサーバとワークステーションの間に同様に調整が必要である。しかしながら、この方法は、より短時間で済むため、EEPROM及びCMOSに有る保護フィールドを上述の第1の方法より、短時間危険にさらすだけで済む。この方法は、メディアレス・ステーションをパワーオフの状態ですター

トさせる必要がある。

【0108】物理的にメディアレス・ワークステーションの直近であれば、承認されたユーザは、上述の第1の方法のようにサーバのユーザに対して論理的起動装置をオペレーティング・システム・イメージからシステム・リファレンス・ディスク・イメージに変更するよう指示する。メディアレス・ワークステーションの承認されたユーザは、それからワークステーションをパワーオンにする。承認されたユーザはこの時、POSTからの可視的表示を待って、鍵盤上で3つの連続打鍵、Ctrl-A

lt-Ins、を行う。この連続打鍵は、POSTに対して、サーバの当該イメージを起動する前に、EEPROMとCMOSの保護フィールドが保護状態になっていない事を知らせるために使用される。

【0109】この状況に於いて、システム・リファレンス・ディスク・イメージが起動され、PAPが導入され、或いはメディアレス・ワークステーションの側から離れる前にシステムがパワーオフされている事を確認するのは、承認されたユーザの責任である。

10 【0110】POSTはビデオ・サブシステムを初期化し、テストとシステム内の他のサブシステムの初期化を行う。これは、メモリ、鍵盤、タイマ、及びDMA制御部を含む。鍵盤サブシステムが初期化されれば、承認されたユーザは該連続打鍵、Ctrl-alt-Ins、を行う事ができる。鍵盤サブシステムが初期化されれば、鍵盤BIOSは、Ctrl-Alt-Ins、の打鍵を業界では有名になっている、Ctrl-Alt-Del、の識別と類似の方法で識別可能になる。この時承認されたユーザに対する可視的表示はなされていない。

20 【0111】POSTは鍵盤のCB IOSをチェックして該打鍵が、鍵盤サブシステムの初期化とPOSTによって該打鍵入力のため、ウィンドウが開かれている事を知らせる可視的合図の送出との間に検出されたかどうか調べる。もし該打鍵がその間に検出されていたら、POSTはシステム区画起動打鍵検出ウィンドウを開かない。もし該打鍵がその間に検出されていなければ、POSTはシステム区画起動打鍵検出ウィンドウを開く。

【0112】POSTはそれから、ディスプレイ上のカーソルを、現在位置、0行0列(左上隅)、から0行79列(上右隅)へ動かす。これは、承認されたユーザにシステム区画起動打鍵検出ウィンドウが開かれている事を知らせるために行われる。次に、POSTはディスク・サブシステムを初期化し、アダプタをオンボード(on-board) ROMと共にシステムに統合するためにアダプタROMスキャンを行い、更にSCSIサブシステムの初期化を行う。

【0113】承認されたユーザが、起動手順中、保護フィールドを露出したままPOSTに知らせるため、該連続打鍵入力、Ctrl-Alt-Ins、をしなければならないのは、このウィンドウの間である。

【0114】この時点で、POSTはシステム区画起動打鍵検出ウィンドウを閉じ、ディスプレイ上のビデオ・カーソルを0行79列(右上隅)から初めの位置、0行0列(左上隅)へ戻す。この事がユーザに対してシステム区画起動打鍵検出ウィンドウが閉じられた事を示す事になる。もし承認されたユーザが、該連続打鍵を入力したとすれば、それが鍵盤の初期化後で、ウィンドウ開の前であっても、或いはウィンドウ開の間中であっても、POSTは、後の使用のため該打鍵の検出を表示するフラグをセットする。

【0115】もし承認されたユーザが、該打鍵入力の場合をのがしたら、その承認されたユーザは、最初に述べた方法に従ってPAPを導入するか、この方法をやり直す事ができる。遠隔IPLに先行して、POSTは該打鍵フラグをチェックし、承認されたユーザがEEPROMとCMOSの保護フィールドを不保護にして置く事を望んでいる事が判る。

【0116】POSTは正常な起動手順を、遠隔IPLの実行が必要であるという事を発見するまで進め、保護フィールド不保護の状態でその手順を進める。第1の方法の説明にあるように、起動イメージが装顔されると、承認されたユーザはセット機構オプションを主メニューの中から選択する。セット機構メニュー上で承認されたユーザはパスワード・ユーティリティを発動するためセット・パスワードと不在開始モード(Unattended Start Mode)を選択する。承認されたユーザはそれから特権アクセス・パスワードを選択し、与えられた指示に従う。該ユーザは同時に、IPL装置起動手順リストを定義し導入する必要がある。

【0117】これによって、承認されたユーザによって選択された起動装置が起動手順中いつも選択されている事が確認される。メディアレス・ワークステーションを離れる前に、承認されたユーザはそのワークステーションのパワーオフをすべきである。さもなければ、もしそのワークステーションがパワーオンのままであると、EEPROMとCMOSの機密保護関係のフィールドが不正なアクセスの危険にさらされる。第1の方法の説明にあるように、この方法はPAPの変更又は削除及びIPLの装置起動手順リストの更新にも使用される。

【0118】POSTによってCtrl-Alt-Ins、の入力のために開かれたウィンドウは、米国特許出願で、1991年6月17日出願の出願番号第716,594号に述べられている。

【0119】そこではそれがシステム・リファレンス・ディスクを起動するために使用されている。本開示に於いては、それが遠隔IPLの為に保護フィールドがロック解除(open)になっている事をPOSTへ知らせるために使用されている。PAPの導入又は変更の処理が、PAPを定義している危険なデータの如何なるネットワーク上の転送も回避しており、それ故該データがネットワーク上に存在する可能性或いはネットワーク上で誤用される可能性を回避しているということが本発明にとって重要である。

【0120】図面と明細書に於いて本発明の望ましい具体化が説明され、特別の用語が使用されているけれど

も、説明は用語を一般的、記述的意識でのみ使用したのであり、制限を加える目的で使用したのではない。

【0121】

【発明の効果】本発明によれば、LANステーション・パーソナル・コンピュータ・システム(固定ディスク装置やフロッピー・ディスク装置のようなプログラム記憶媒体を持たない)において、パスワード・データの如何なるネットワーク上の転送も回避し、それ故該データがネットワーク上に存在する可能性或いはネットワーク上で誤用される可能性を回避することができ、LAN上での機密保護機能を提供することができる。

【図面の簡単な説明】

【図1】本発明を具体化する場合のパーソナル・コンピュータの外観図である。

【図2】図1のパーソナル・コンピュータの構成要素で、シャシ、カバー、プレーナ・ボードを含む分解部品配置図であり、これら構成要素の関係を示している。

【図3】図1及び図2のパーソナル・コンピュータの特定部分の概略図である。

【図4】図1及び図2のパーソナル・コンピュータの特定の構成部分で、本発明の機密保護に関連した部分を概略示したものである。

【図5】図1及び図2のパーソナル・コンピュータの特定の構成部分で、本発明の機密保護に関連した部分を概略示したものである。

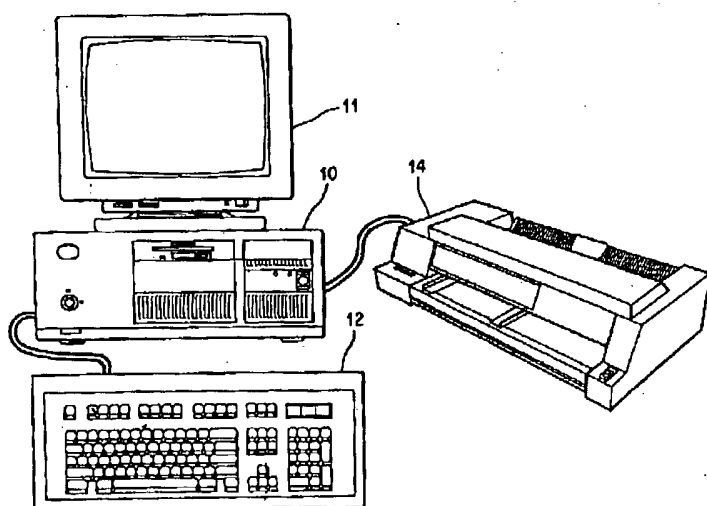
【図6】図4及び図5で表示された特定の構成部分の拡大外観図である。

【図7】本発明の機密保護機構に関連する図1、図2、図4及び図5で示されるパーソナル・コンピュータのオプション部分の拡大外観図である。

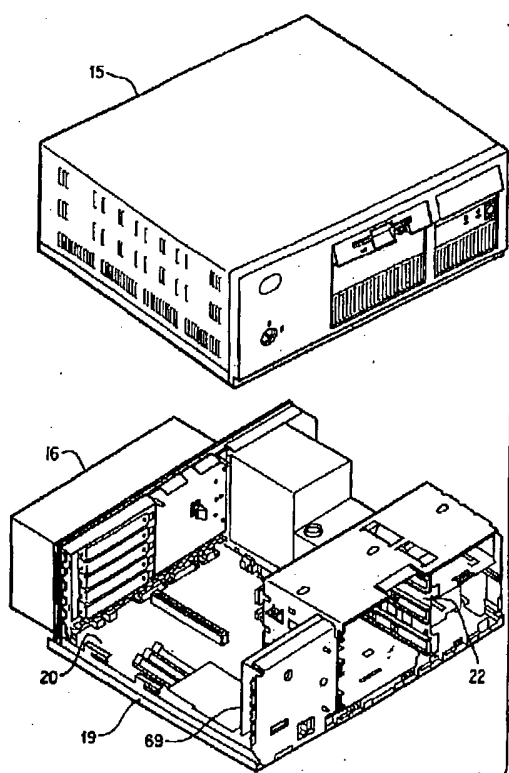
【符号の説明】

- 10 パーソナル・コンピュータ
- 11 ディスプレイ・モニタ
- 12 鍵盤
- 15 主カバー
- 19 シャシ
- 20 プレーナ・ボード
- 36 SIMMS (RAM)
- 38 BIOS ROM
- 59 EEPROM
- 61 電源スイッチ
- 62 電源
- 64 カバー錠スイッチ
- 68 RTC/CMOS RAM

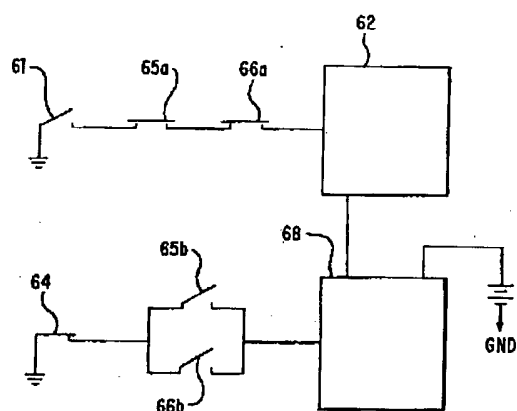
【図1】



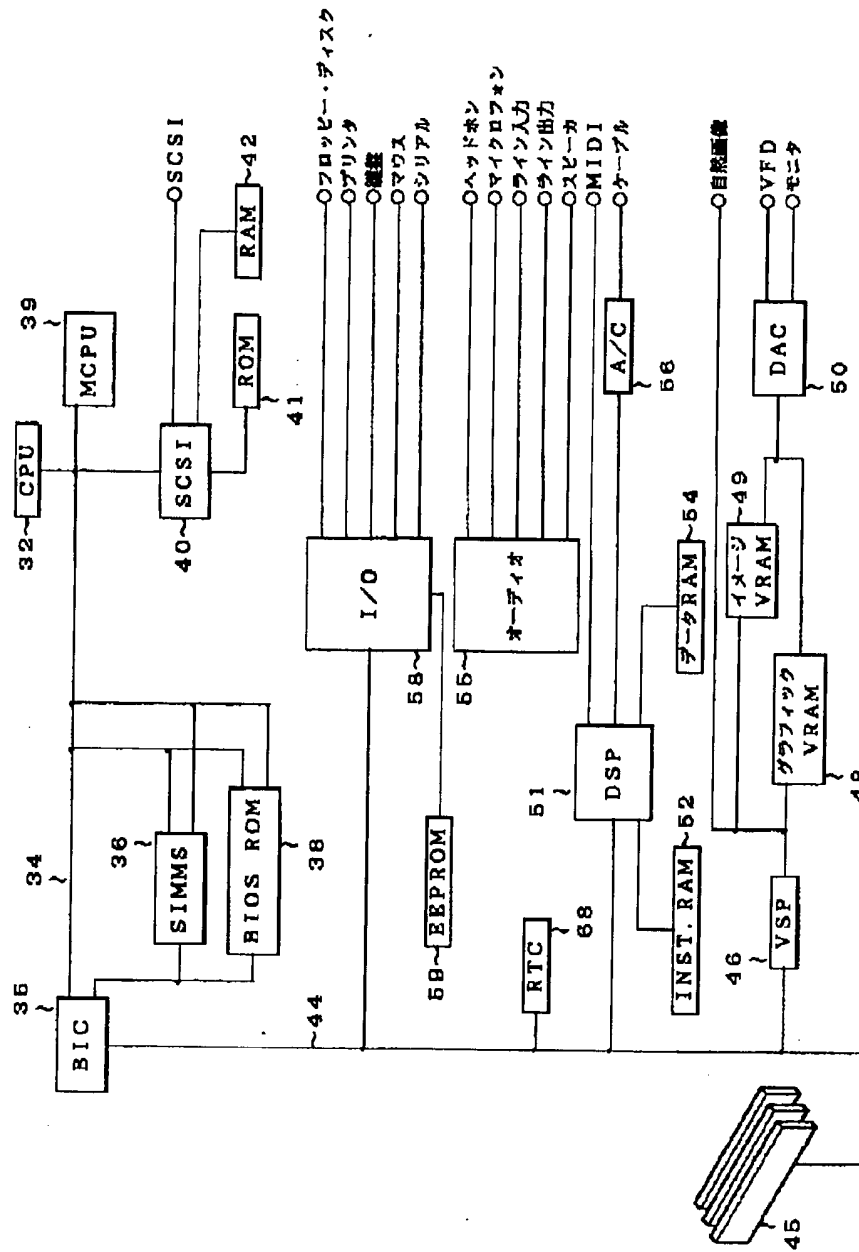
【図2】



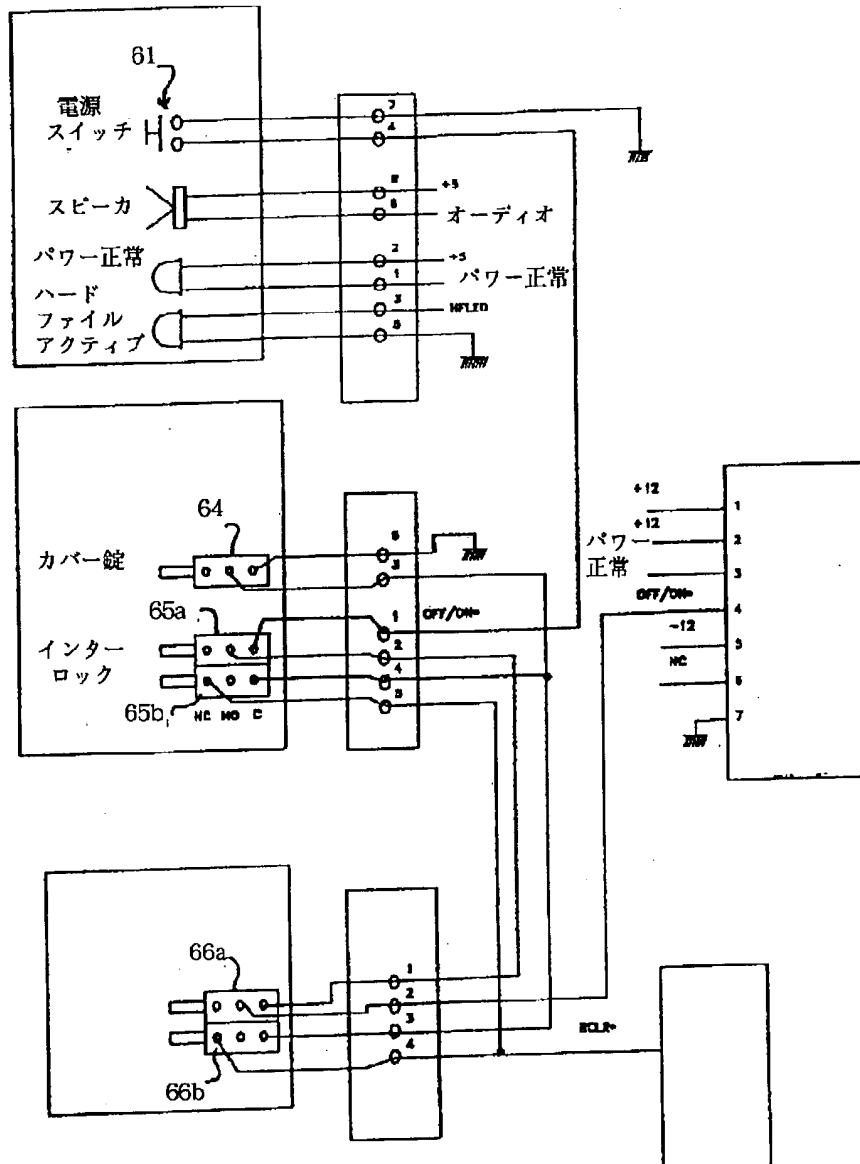
【図4】



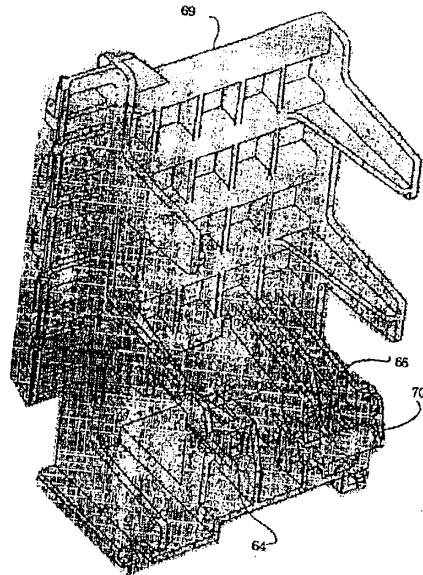
【図3】



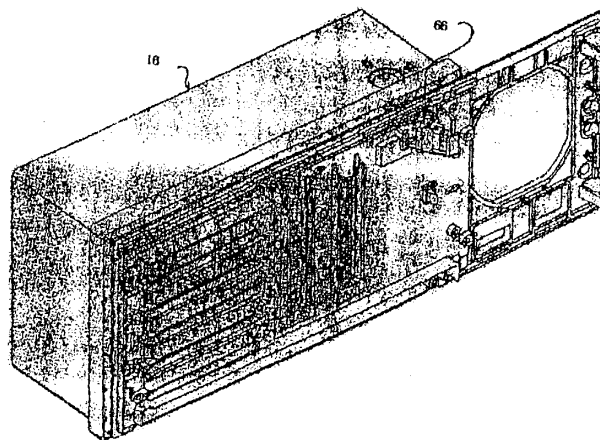
【図5】



【図6】



【図7】



フロントページの続き

(72)発明者 キムサン・ド・レ
アメリカ合衆国 33437 フロリダ州・ポ
イントン・ビーチ サン・ポイント・ドラ
イブ 9422

(72)発明者 マッシュウ・テイー・ミッテルステッド
アメリカ合衆国 30144 ジョウジア州・
ケネソウサンダーリングス・ポイント
3550

(72)発明者 パーマー・イー・ニューマン
アメリカ合衆国 33433 フロリダ州・ボ
カラトンダブリン・ドライブ 7488

(72)発明者 デーブ・リー・ランドール
アメリカ合衆国 33068 フロリダ州・ボ
ンパノ・ビーチ 69テラス 1751 エス・
ダブリュウ

(72)発明者 リサ・アンネ・ルオトロ
アメリカ合衆国 33467 フロリダ州・レ
イク・ワース アウアチタ・ドライブ
5264

(72)発明者 ジョアンナ・バーガー・ヨダ
アメリカ合衆国 27513 ノースカロライ
ナ州・ケアリー カスター・トレイル
203